

ABSTRACT

An anti malware scanner for files is provided with means for processing script and macro files and flagging them as suspect or not based upon an automated analysis of source code in the file. This analysis involves separating the program source into groups of parts such as comment, variable names and routine names, eliminating duplicates and performing a character frequency distribution analysis of the resulting strings. The system may include an exception list to omit flagging a file as suspect if it is on the exception list.